

Zur Lehre von den Modulargleichungen der elliptischen Functionen.

Von Dr. G. Pick,
Privatdocent in Prag.

(Vorgelegt in der Sitzung am 8. Jänner 1885.)

Im Verlaufe von Untersuchungen über die complexe Multiplication der elliptischen Functionen haben sich mir gewisse zahlentheoretische Eigenschaften der Coëfficienten der Modulargleichungen dargeboten, welche trotz ihrer einfachen Gesetzmässigkeit und der geringen Schwierigkeiten ihrer Herleitung noch nicht bemerkt worden zu sein scheinen. Ich theile dieselben im Folgenden mit und schicke nur eine kurze Übersicht über die wenigen, übrigens wohlbekannten Sätze und Entwickelungen voraus, welche zu ihrer Aufstellung nöthig erscheinen.

1.

Als Modul verwenden wir ausschliesslich die Grösse

$$x(\omega) = 4^4 \frac{(1-k^2+k^4)^3}{k^4(1-k^2)^2}$$
$$= 1728 \cdot J,$$

wo k den gewöhnlich so genannten Modul des Legendre'schen Normalintegrals

$$\int \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}},$$

also J die „absolute Invariante" [1] bedeutet. Die Grösse $x(\omega)$ hängt von dem Periodenquotienten ω des Integrals

---

[1] Die Grösse $\frac{g_2^3}{g_2^3-27g_3^2}$ nach der von Herrn Weierstrass eingeführten Bezeichnungsweise. Vgl. F. Klein, Math. Ann. Bd. 14, S. 112 ff.

$$\int \frac{du}{\sqrt{u(1-u)(1-k^2u)}}$$

derartig ab, dass sie ungeändert bleibt, wenn man ω durch

$$\frac{\gamma+\delta\omega}{\alpha+\beta\omega}$$

ersetzt, wofern $\alpha, \beta, \gamma, \delta$ ganze Zahlen sind mit der Determinante

$$\alpha\delta-\beta\gamma = 1.$$ [1]

Bedeuten a, b, c, d vier ganze Zahlen, deren Determinante

$$ad-bc = n$$

positiv und grösser als 1 ist, so bezeichnet man den Übergang von ω zu

$$\varpi = \frac{c+d\omega}{a+b\omega}$$

als Transformation n^{ter} Ordnung. Denkt man sich alle möglichen (unendlich vielen) Transformationen n^{ter} Ordnung ausgeführt, und von jedem erhaltenen ϖ die Function $x(\varpi)$ gebildet, so ergibt sich doch nur eine endliche Zahl von einander verschiedener Grössen $x(\varpi)$, welche man sämmtlich, und zwar jede nur einmal erhält, indem man ϖ alle Werthe von der Form

$$\frac{C+D\omega}{A}$$

ertheilt, wobei A und D positive ganze Zahlen bedeuten, deren Product

$$A.D = n$$

ist, und C jeden Werth eines vollständigen Restsystems (mod. A) erhält, also am einfachsten jedesmal die Zahlen

$$0, 1, 2, \ldots, A-1$$

durchläuft. [2]

---

[1] Vgl. F. Klein, a. a. O.

[2] Vgl. z. B. Königsberger, Theorie der elliptischen Functionen (Leipzig), Bd. II., S. 43 ff.

Die sämmtlichen Grössen

$$x(\varpi) = x\left(\frac{C+D\omega}{A}\right)$$

bilden die Wurzeln einer algebraischen Gleichung

$$F_n(x, y) = \prod_{\varpi} [y - x(\varpi)] = 0,$$

deren höchster Coëfficient gleich Eins, deren übrige ganze rationale Functionen von x sind. Diese Gleichung kann als „reducible" Modulargleichung[1] für den n^{ten} Transformationsgrad bezeichnet werden im Gegensatze zu jenen eigentlichen (irreduciblen) Modulargleichungen, welche man erhält, indem man von den „Repräsentanten"

$$\frac{C+D\omega}{A}$$

alle jene ausschliesst, in welchen A, C, D einen gemeinsamen Theiler besitzen.

Die Function $x(\omega)$ besitzt eine Reihenentwickelung nach Potenzen von

$$Q = e^{2\pi i\omega}$$

von der Form

$$x(\omega) = \frac{1}{Q}(1 + \gamma_1 Q + \gamma_2 Q^2 + \cdot \quad \cdot), \tag{1}$$

in welcher $\gamma_1, \gamma_2,$ ganze rationale Zahlen bedeuten, auf deren specielle Werthe es übrigens im Folgenden nicht ankommt.

Ausser diesen der Theorie der elliptischen Functionen angehörigen Begriffen und Entwickelungen werden im Folgenden noch zwei der Zahlentheorie entnommene Sätze zur Verwendung gelangen, welche kurz Erwähnung finden mögen.

1. Wenn $\alpha, \beta, \ldots, \mu$ die Wurzeln einer algebraischen Gleichung bedeuten, deren höchster Coëfficient gleich Eins, deren

---

[1] Vgl. Hurwitz, Göttinger Nachrichten, 1883, 21. Nov.

übrige ganze rationale Zahlen sind, so ist bekanntlich jede ganze, mit ganzzahligen Coëfficienten versehene symmetrische Function jener Wurzeln

$$s(\alpha, \beta, \ldots, \mu)$$

eine ganze Zahl.

Bedeutet nun p eine beliebige Primzahl, so findet die Congruenz statt:

$$s(\alpha^p, \beta^p, \ldots, \mu^p) \equiv s(\alpha, \beta, \ldots, \mu) \quad (\text{mod. } p).$$

Durch wiederholte Anwendung dieses Satzes erhält man:

$$s(\alpha^{p^k}, \beta^{p^k}, \ldots, \mu^{p^k}) \equiv s(\alpha, \beta, \ldots, \mu) \quad (\text{mod. } p).$$

Den höchst einfachen Beweis dieses Satzes findet man zum Beispiel in der Abhandlung von Herrn Dedekind: „Beweis für die Irreducibilität der Kreistheilungsgleichungen" (Crelle's Journal, Bd. 54, S. 28).[1]

2. Bedeutet $f(x, y, \ldots, t)$ eine mit ganzzahligen Coëfficienten versehene Function der unbestimmten Grössen $x, y, \ldots, t$, so findet die identische Congruenz statt:

$$f(x^p, y^p, \ldots, t^p) \equiv f(x, y, \ldots, t,)^p \quad (\text{mod. } p),$$

aus welcher sich durch wiederholte Anwendung ergibt:

$$f(x^{p^k}, y^{p^k}, \ldots, t^{p^k}) \equiv f(x, y, \ldots, t)^{p^k} \quad (\text{mod. } p).$$

Dieser Satz ist in kaum weniger allgemeiner Form schon von Gauss angewendet worden. (Gauss' Werke, Bd. II, S. 227.)

2.

Es soll nun vor Allem bewiesen werden, dass das im vorigen Paragraphen mit $F_n(x, y)$ bezeichnete Polynom lauter ganze rationale Zahlen zu Coëfficienten besitzt.

Es sei

$$\bar{Q} = e^{2\pi i \bar{\omega}};$$

---

[1] Vgl. auch Gauss' Werke, Bd. II, S. 224.

dann ist

$$x(\bar{\omega}) = \frac{1}{\bar{Q}}(1+\gamma_1\bar{Q}+\gamma_2\bar{Q}^2+\ldots),$$

und folglich

$$F_n(x, y) = (-1)^{\Sigma A}.\prod_{\bar{Q}}\frac{1}{\bar{Q}}(1+[\gamma_1-y]\bar{Q}+\gamma_2\bar{Q}^2+\ldots),$$

führt man nun für $\bar{Q}$ seinen Ausdruck

$$e^{2\pi i\frac{C+D\omega}{A}} = e^{\frac{2\pi i C}{A}}.Q^{\frac{D}{A}}$$

ein, so kann das Product in der folgenden Weise ausgeführt werden. Man multiplicire zunächst bei festgehaltenem A über alle Werthe 0, 1, $\ldots$ $A-1$ der Grösse C. Hiedurch erhält man für jeden Werth von A je ein Theilproduct, welches nur mehr ganze Potenzen von Q enthält, und offenbar nur eine endliche Anzahl von negativen Potenzen dieser Grösse; die Coëfficienten der einzelnen Potenzen aber sind ganze und ganzzahlige Functionen von y. Insbesondere wird das erste Glied der Entwickelung (also dasjenige mit der niedrigsten Potenz von Q)

$$\prod_{C=0}^{A-1}\frac{1}{e^{\frac{2\pi i C}{A}}.Q^{\frac{D}{A}}} = (-1)^{A+1}\frac{1}{Q^D}.$$

Alles dies folgt aus den elementarsten Betrachtungen über symmetrische Functionen, und ist aus dem blossen Anblick jedes solchen Theilproductes klar.

Multiplicirt man nun alle auf solche Weise gebildeten Theilproducte mit einander, so resultirt eine Gleichung von der Form

$$F_n(x, y) = (-1)^g\frac{1}{Q^N}\{1+Y_1.Q+Y_2.Q^2+\ldots\};$$

hierin bedeutet g die Anzahl aller Theiler der Zahl n, $N = \Sigma D$ die Summe aller dieser Theiler; durch Y_1, Y_2, $\ldots$ endlich sind ganze Functionen von y bezeichnet mit ganzzahligen Coëfficienten. Auch dies ist aus der Entstehungsweise jenes Ausdrucks unmittelbar ersichtlich.

Es gelten nun für jede Potenz der Grösse $x = x(\omega)$ Entwickelungen von folgender Gestalt:

$$x^m = \frac{1}{Q^m}(1+\gamma_1^{(m)}Q+\gamma_2^{(m)}Q^2+\ldots),$$

(worin $\gamma_1^{(m)}, \gamma_2^{(m)}, .$ ganze Zahlen bedeuten), wie aus Formel (1) der vorigen Paragraphen hervorgeht. Bringt man also die Grösse $(-1)^g . x^N$ von $F_n(x, y)$ in Abzug, so ergibt sich

$$F_n(x, y)-(-1)^g x^N = \frac{1}{Q^{N-1}}\{Y'+Y_1'.Q+Y_2'Q^2+. \;.\},$$

wo nun Y', Y_1', Y_2' wieder ganze und ganzzahlige Functionen von y bedeuten. Man wird nun weiter den Ausdruck

$$F_n(x, y)-(-1)^g x^N-Y'x^{N-1} = \frac{1}{Q^{N-2}}\{Y''+Y_1''Q+Y_2''Q^2+ \quad .\}$$

bilden, wobei Y'', Y_1'', Y_2'' abermals Grössen von der Eigenschaft der Y sein werden und in derselben Weise fortfahren, um endlich eine Gleichung von der Form zu erhalten:

$$F_n(x, y)-(-1)^g x^N-Y'.x^{N-1}-. \;.-Y^{(N-1)}.x$$
$$= Y^{(N)}+Y_1^{(N)}.Q+Y_2^{(N)}.Q^2+..$$

Nun aber ist leicht zu zeigen, dass sich die rechte Seite auf $Y^{(N)}$ allein reduciren muss. Denn linkerhand steht eine ganze rationale Function von x (welche ausserdem den Parameter y enthält), die also nur für $x = \infty$, das heisst für $Q = 0$, einen unendlich grossen Werth erlangen kann. Für $Q = 0$ aber convergirt die rechte Seite unserer Gleichung gegen einen endlichen Werth, weil negative Potenzen von Q nicht vorhanden sind. Also muss sie überhaupt von Q unabhängig sein. Unser Resultat lautet somit

$$F_n(x, y) = (-1)^g x^N+Y'x^{N-1}+Y''x^{N-2}+\ldots+Y^{(N)};$$

aus der wiederholt angegebenen Beschaffenheit der Functionen Y ergibt sich der im Eingang dieses Paragraphen ausgesprochene Satz.

Es sei noch bemerkt, dass $(-1)^g$ dann und nur dann gleich -1 ist, wenn n eine Quadratzahl ist. Denn die Theiler von n lassen sich so in Paare ordnen, dass jedes Paar n selbst als Product ergibt; nur in dem Falle eines vollständigen Quadrats bleibt ein Theiler $(\sqrt{n})$ übrig.

Wir wollen nun die Modulargleichung vom n^{ten} Transformationsgrade mit derjenigen für die Transformation von der Ordnung $p^\lambda n$ in Beziehung setzen, wobei p eine in n nicht enthaltene Primzahl, λ eine beliebige positive ganze Zahl bedeutet.

Bildet man ein vollständiges System von Repräsentanten für die Transformation $p^{\lambda\text{ter}}$ Ordnung, und unterwirft jeden derselben sämmtlichen Transformationen n^{ter} Ordnung, so erhält man bekanntlich ein vollständiges Repräsentantensystem für den Transformationsgrad $p^\lambda n$.

In der That, setzt man in dem Ausdrucke

$$\varpi = \frac{C+D\omega}{A}$$

für ω irgend eine Grösse von der Form

$$\frac{K+p^{\lambda-\rho}\,.\,\omega}{p^\rho},$$

so geht ϖ über in

$$\bar{\varpi} = \frac{(Cp^\rho+DK)+p^{\lambda-\rho}D\,.\,\omega}{p^\rho A}.$$

Hierin ist

$$(p^\rho A)\times(p^{\lambda-\rho}D) = p^\lambda n;$$

und lässt man C die Werthe

$$0, 1, \ldots, A-1,$$

und unabhängig davon K die Werthe

$$0, 1, \quad ., p^\rho-1$$

durchlaufen, so nimmt der Ausdruck

$$Cp^{\rho}+DK$$

jeden Werth eines vollständigen Restsystems (mod. Ap^{ρ}) einmal und nur einmal an, wie in den Elementen der Zahlentheorie gezeigt wird.

Um also aus der Modulargleichung

$$F_{n}(x,y)=0$$

die neue

$$F_{p^{\lambda}n}(x,y)=0$$

zu erhalten, hat man in $F_{n}(x,y)$ für x sämmtliche Grössen

$$x\left[\frac{K+p^{\lambda-\rho}\omega}{p^{\rho}}\right]$$

einzusetzen, und die entstandenen Polynome miteinander zu multipliciren.

So erhält man

$$F_{p^{\lambda}n}(x,y)=\prod_{\rho,K}F_{n}\left(x\left[\frac{K+p^{\lambda-\rho}\omega}{p^{\rho}}\right],\ y\right)$$

$$=(-1)^{g(\lambda+1)}\prod_{\rho,K}\frac{1}{Q^{N}_{\rho,K}}\{1+Y_{1}Q_{\rho.K}+Y_{2}Q^{2}_{\rho,K}+\ldots\}.$$

Hierin bedeutet $Q_{\rho,K}$ die Grösse

$$e^{2\pi i\frac{K+p^{\lambda-\rho}\omega}{p^{\rho}}}=e^{\frac{2\pi iK}{p^{\rho}}}\quad Q^{p^{\lambda-2\rho}}$$

Wir zerlegen nun den gefundenen Ausdruck für $F_{p^{\lambda}n}(x,y)$ in Theilproducte, indem wir zunächst bei festgehaltenem ρ über alle

$$K=0,1,\ \ldots,p^{\rho}-1$$

multipliciren. Hier treten nun die beiden am Schlusse des ersten Paragraphen aufgeführten zahlentheoretischen Sätze in Kraft.

Nach dem ersten derselben ersetzen wir die in den Factoren vorkommenden Einheitswurzeln

$$e^{\frac{2\pi iK}{p^{\rho}}}$$

sämmtlich durch ihre $p^{\rho \text{ten}}$ Potenzen, das heisst durch

$$+1.$$

Hiedurch geht das Product über in

$$(-1)^{g(\lambda+1)} \prod_{\rho} \left\{ \frac{1}{Q^{Np^{\lambda}-2\rho}} \left[1 + Y_1 Q^{p^{\lambda}-2\rho} + Y_2 Q^{2p^{\lambda}-2\rho} + \dots\right] \right\}^{p^{\rho}}.$$

Nun führen wir mit Hilfe des zweiten Satzes die Potenz unter dem Productzeichen aus, wodurch wir erhalten:

$$(-)^{g(\lambda+1)} \prod_{\rho} \left\{ \frac{1}{Q^{Np^{\lambda}-\rho}} \left[1 + Y_1^{p^{\rho}} Q^{p^{\lambda}-\rho} + Y^{p^{\rho}} Q^{2p^{\lambda}-\rho} + \dots\right] \right\}.$$

Der jetzt unter dem Productzeichen stehende Ausdruck entsteht nun augenscheinlich aus

$$(-1)^g F_n(x, y) = \frac{1}{Q^N}\left[1 + Y_1 Q + Y_2 Q^2 + \dots\right],$$

indem man hierin für y überall $y^{p^{\rho}}$, für Q aber $Q^{p^{\lambda}-\rho}$ einsetzt. Denkt man also jenen Ausdruck nach Potenzen von $y^{p^{\rho}}$ geordnet, so sind die einzelnen Coëfficienten dieser Potenzen nach dem zweiten Hilfssatze durch die $p^{\lambda-\rho \text{ten}}$ Potenzen der entsprechenden Coëfficienten in $(-1)^g F_n(x, y)$ zu ersetzen. Das heisst aber, wir werden auf die Grösse

$$(-1)^g F_n(x^{p^{\lambda-\rho}}, \; y^{p^{\rho}})$$

geführt. Fassen wir alle diese Umgestaltungen zusammen, so können wir sagen: das zum Index ρ gehörige Theilproduct weicht von der Grösse

$$(-1)^g F(x^{p^{\lambda-\rho}}, y^{p^{\rho}})$$

um eine Reihe in Q ab, deren Coëfficienten ganze Functionen von y sind, welche selbst ganzzahlige Coëfficienten tragen, deren jeder durch p theilbar ist.

Führen wir nun auch die Multiplication nach ρ aus, so ergibt sich

$$F_{p^\lambda n}(x, y) = \prod_{\rho=0}^{\lambda} F_n(x^{p^{\lambda-\rho}}, y^\rho) + p \cdot \{Q, y\},$$

worin durch $\{Q, y\}$ eine Reihe nach Q bezeichnet ist, deren Coëfficienten ganze und ganzzahlige Functionen von y sind.

Aber diese Reihe muss selbst eine ganze Function von x und y sein, weil sowohl $F_{p^\lambda n}(x, y)$ als auch das rechts stehende Product solche Functionen sind. Sie muss ferner durchaus ganze Zahlen als Coëfficienten der einzelnen Posten besitzen, was augenscheinlich in Überlegungen genau derselben Art seinen Grund hat, wie sie im zweiten Paragraphen an $F_n(x, y)$ durchgeführt worden sind.

Wir haben es also in unserer Schlussgleichung mit lauter ganzen und ganzzahligen Polynomen in x und y zu thun, und können daher mit Benützung des Congruenzzeichens einfacher schreiben:

$$F_{p^\lambda n} \equiv \prod_{\rho=0}^{\lambda} F_n(x^{p^{\lambda-\rho}}, y^\rho) \pmod{p}.$$

Unter abermaliger Benützung jenes zweiten zahlentheoretischen Hilfssatzes können wir diese Formel für ungerade λ in die Gestalt setzen

$$F_{p^\lambda n}(x, y) \equiv \prod_{0 \leqq \rho < \frac{\lambda}{2}} \{F_n(x^{p^{\lambda-2\rho}}, y) \cdot F_n(x, y^{p^{\lambda-2\rho}})\}^{p^\rho};$$

für gerade λ tritt zu dem Producte rechterhand noch der Factor

$$F_n(x, y)^{p^{\frac{\lambda}{2}}}$$

4.

Der im vorigen Paragraphen gefundene Satz verliert seine Giltigkeit nicht, wenn $n = 1$ gesetzt wird.

An Stelle der Modulargleichung $F_n(x, y) = 0$ tritt dann einfach die Gleichung

$$y - x = 0.$$

Wir erhalten also die Formel

$$F_{p^\lambda}(x, y) \equiv \prod_{\rho=0}^{\lambda} (y^{p^\rho} - x^{p^{\lambda-\rho}}) \quad (\text{mod. } p).$$

Ist insbesondere $\lambda = 1$, so wird

$$F_p(x, y) \equiv (y - x^p)(y^p - x) \quad (\text{mod. } p).$$

Es gibt also nur vier Glieder in der Modulargleichung von der Primzahlordnung p, deren Coëfficienten nicht durch p theilbar sind, nämlich die Glieder mit

$$y^{p+1},\ x^p y^p,\ xy,\ x^{p+1}.$$

Wir fügen nun noch eine Bemerkung hinzu. Dasselbe Verfahren, welches uns gedient hat, um zahlentheoretische Eigenschaften der Coëfficienten der reduciblen Modulargleichungen aufzufinden, kann angewendet werden, um in gleicher Weise über die Beschaffenheit der irreduciblen Modulargleichungen ins Klare zu kommen.

Aber man kann auch von den hier gefundenen Congruenzen direct zu solchen übergehen, welche für die irreduciblen Modulargleichungen Geltung haben. Bedeutet nämlich $\Phi_n(x, y)$ die gewöhnlich so genannte Modulargleichung für den $n$ten Transformationsgrad, so ist bekanntlich

$$F_n(x, y) = \prod_a \Phi_{\frac{n}{a^2}}(x, y),$$

wobei das Product über alle Zahlen a zu erstrecken ist, deren Quadrate in n aufgehen. Aus dieser Gleichung erhält man nach einer allgemeinen Auflösungsmethode, welche von Herrn Dedekind angegeben worden ist,[1] umgekehrt Φ_n ausgedrückt durch verschiedene Polynome F_n. Durch geeignete Verbindung der oben gefundenen Congruenzen können dann offenbar analoge für Φ_n gefunden werden.

---

[1] Crelle's Journal, Bd. 54, S. 25 f. oder Dirichlet-Dedekind Zahlentheorie (3. Aufl.), S. 362.

Ohne auf diese Ableitung, welche vollkommen elementar ist und kein weiteres Interesse bietet, näher einzugehen, setze ich noch die Hauptformel her, welche man zum Schlusse erhält. Es ergibt sich

$$\Phi_{p^\lambda n}(x, y) \equiv \prod_{0 \leqq \rho < \frac{\lambda}{2}} \left\{\Phi_n(x^{p^{\lambda-2\rho}}, y) \cdot \Phi_n(x, y^{p^{\lambda-2\rho}})\right\}^{\varphi(p^\rho)}$$

für ungerade λ; für gerade λ tritt auf der rechten Seite noch der Factor

$$\Phi_n(x, y)^{\varphi\left(p^{\frac{\lambda}{2}}\right)}$$

hinzu. $\varphi(k)$ bedeutet dabei die bekannte Gauss'sche Function.